51. IWK

Internationales Wissenschaftliches Kolloquium
International Scientific Colloquium

PROCEEDINGS 11-15 September 2006

FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION SCIENCE

INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING - DEVICES AND SYSTEMS, MATERIALS AND TECHNOLOGIES FOR THE FUTURE

Startseite / Index:
http://www.db-thueringen.de/servlets/DocumentServlet?id=12391

TECHNISCHE UNIVERSITÄT
ILMENAU

Impressum

Herausgeber: Der Rektor der Technischen Universität Ilmenau
Univ.-Prof. Dr. rer. nat. habil. Peter Scharff

Redaktion: Referat Marketing und Studentische Angelegenheiten
Andrea Schneider

Fakultät für Elektrotechnik und Informationstechnik
Susanne Jakob
Dipl.-Ing. Helge Drumm

Redaktionsschluss: 07. Juli 2006

Technische Realisierung (CD-Rom-Ausgabe):
Institut für Medientechnik an der TU Ilmenau
Dipl.-Ing. Christian Weigel
Dipl.-Ing. Marco Albrecht
Dipl.-Ing. Helge Drumm

Technische Realisierung (Online-Ausgabe):
Universitätsbibliothek Ilmenau
ilmedia
Postfach 10 05 65
98684 Ilmenau

Verlag:
Verlag ISLE, Betriebsstätte des ISLE e.V.
Werner-von-Siemens-Str. 16
98693 Ilrnenau

ISBN (Druckausgabe): 3-938843-15-2
ISBN (CD-Rom-Ausgabe): 3-938843-16-0

Startseite / Index:
http://www.db-thueringen.de/servlets/DocumentServlet?id=12391

51st Internationales Wissenschaftliches Kolloquium
Technische Universität Ilmenau
September 11 – 15, 2006

A. Diab, A. Mitschele-Thiel, R. Boeringer

Integration between MIFA and HMIP to Support Fast Inter-domain Mobility in IP Networks

ABSTRACT

It is nowadays well known that All-IP networks will be the future B3G networks. However, in order to make these networks as good as 2 or 3G networks with respect to the performance, many challenges have to be faced. One of the main challenges is the developing of suitable mobility solutions to support seamless and fast movement in the network. **M**obile **IP** (MIP) presents the standard mobility management protocol. However, MIP is not adequate for delay sensitive applications. Therefore, micro mobility management solutions are introduced to process the movements locally. Micro mobility divides the space the MN moves inside into domains. The MN performs intra-domain handoff when moving inside the domain and inter-domain handoff when moving between different administrative domains. Standard Frameworks use a micro mobility solution to support intra-domain mobility and MIP to support inter-domain handoffs.

Mobile **I**P **F**ast **A**uthentication protocol (MIFA) is proposed to avoid the problems of MIP and to match the requirements of real-time applications. Our performance studies have shown that MIFA clearly outperforms MIP with respect to the handoff latency and the expected number of the dropped packets. Thus, it is useful to integrate MIFA with other micro mobility protocols to support fast intra- and inter-domain mobility.

In this paper we propose a new mobility management framework. This framework integrates **H**ierarchical **M**obile **IP** (HMIP) as a micro mobility management protocol with MIFA instead of MIP as a macro mobility management protocol. Our proposal should clearly outperform the standard framework with respect to the handoff latency and the expected number of dropped packets during inter-domain handoffs. Inter-domain mobility is accelerated to be approximately the same as intra-domain mobility. The full specification of this framework is presented in this paper.

I- INTRODUCTION

It is nowadays well known that All-IP networks will be the future B3G networks. However, in order to make these networks as good as 2 or 3G networks with respect to performance, many challenges have to be faced. One of the main challenges is how to manage the mobility of the MNs and how to achieve a fast and smooth movement from one point of attachment to another.

Numerous solutions to reduce the handoff latency during the movement between the cells are proposed. These proposals can be broadly classified into four groups. The first group supports global mobility, referred to as macro mobility too. The second one aims at the reduction of the time required to register with the network by processing the handoff procedure locally, e.g. using a hierarchical network architecture. This group divides the space, the MN moves inside, into domains and process the handoff locally inside the domain. This processing is called micro mobility management. The third group attempts to reduce the address resolution time by employing layer2 information to accelerate the layer3 handoff. The fourth group tries to accelerate the micro mobility management by employing layer2 information through combining the solutions of the third group with the solutions of the second one.

The rest of this paper is organized as follows: In section (II) we provide the background and the related work. **M**obile **I**P **F**ast **A**uthentication protocol (MIFA) is presented in section (III). Our proposal is detailed in section (IV). After that we conclude with the main results and the future work in section (V).

II- RELATED WORK

Mobile IP version 4 (MIPv4) [1], [2] or version 6 (MIPv6) [3] present the well known standard to support mobility in IP networks. Using these protocols the MN has to register and to authenticate itself by the **H**ome **A**gent (HA) every time it moves from one subnet to another. This introduces extra latency to the communication, especially when HA is far away from the **F**oreign **A**gent (FA). Additionally, the generation of secret keys [4] for the security association between the HA and the current FA, and/or between the current FA and the MN is another reason for latency. Even though this is optional with

MIP, it is highly recommended for security reasons. In addition, these keys are mandatory for some extensions of MIP, e.g. MIPv4 with routing optimization [5]. The latency experienced by MIP makes it inadequate for the delay sensitive applications. Thus, MIP belongs to the first group, which is only suitable for the management of global (macro) mobility.

In order to avoid these sources of extra latency, several approaches to support micro mobility have been proposed. In [6] an approach to use an **A**nchor **FA** (AFA) has been proposed. If the MN is away from the home network, it will be initially registered by the HA. During this registration a shared secret between the MN and the FA ($K_{MN\text{-}FA}$) is established. The FA then acts as an AFA. Thus, in subsequent registrations, the MN is registered at this AFA instead of the HA as long as it remains in the same domain the AFA belongs to. In this approach there is no need to generate more secret keys to authenticate the MN, and no need to establish a tunnel between the HA and the current FA. Instead, an additional bidirectional tunnel from the AFA to the current FA is established. However, the forwarding delay of the downlink as well as the uplink, i.e. the path from HA via AFA and current FA to the MN and vice versa, increases compared to MIP. Additionally, a tunnel from the previous FA to the current one is required in case the smooth handoff is supported [7].

In [8] a Regional Registration for MIPv4 (HMIPv4) and in [9] Hierarchical Mobile IPv6 (HMIPv6) have been proposed. With these protocols the HA is not aware of every change of the point of attachment. This is due to the fact that the handoff procedures are processed locally by a special node, e.g. a **G**ateway **F**oreign **A**gent (GFA) or **M**obility **A**nchor **P**oint (MAP), when the MN moves inside a certain domain. Thus, the MN communicates with the HA only if it changes this special node. However these protocols require hierarchical network architecture and normally suffer from the single point of failure.

In [10] Proposals for low latency handoffs are proposed. They belong to the third group of mobility management solutions depicted above and use a trigger originating from layer 2 (L2-trigger) to anticipate handoffs prior to a break of the radio link. These methods are pre-registration, post-registration and combined method.

Pre-registration method relies on a L2-trigger fired when a movement to a new sub-network must be achieved. This trigger contains the IP address of the new FA or another address from which the IP address can be derived, e.g. the MAC address, see

[10]. L2-trigger prompts the MN to register with the new FA through the old one. Other words the layer3 handoff is performed while the MN performs a layer2 handoff. The L2-trigger may be fired not only by the MN, but also by the current FA or even the new one, see [10].

In the post-registration method the MN performs only a layer2 handoff, when the L2-trigger is fired. If the link between the current FA and the MN breaks down (receiving a **L**ayer**2 L**ink **D**own trigger – L2-LD), a bidirectional tunnel is established between the old FA and the new one. As a result the packets destined to the MN will be forwarded to the new FA through the old one. When the layer2 handoff is completed, the MN can register with the new FA while receiving the packets. This means that the post-registration method enables the MN to receive the packets before the registration.

With the combined method, the MN first tries to use the pre-registration method when a L2-trigger is received. If this fails, the MN employs the post-registration method to ensure a smooth handoff.

The performance studies and of pre- and post-registration method [11], [12], [13] have shown that the timing of the triggers has a major influence on the handoff latency as well as the packet lose rate. Increased latency results if the L2-trigger for pre-registration is delayed. In case the Registration Request message is dropped, it is possible that this method resorts to the standard layer3 handoff methods, e.g. MIP or HMIP. In addition, the causes for latency of MIP still remain which is due to the forwarding delay between the FA and the HA. Even though post-registration is faster than pre-registration, the impact of delayed L2-triggers with post-registration is the same as with pre-registration. Due to the missing MIP registration with the post-registration approach, the packet delay is larger (uplink and downlink). The combined method inherits the problems of both approaches.

In order to avoid the negative impact of timing problems, an improved approach has been proposed in [14]. In this approach the MN informs the current FA about the movement and registers with the new FA through the old one, similar to the pre-registration approach. However, the old FA forwards the packets directly to the new FA without waiting for a L2-LD trigger. This makes the negative impact of the timing of the L2-trigger smaller than with the other methods.

Fast **M**obile **IP v**ersion **6** (FMIPv6) [15] is another well known example of the third group of mobility management solutions. FMIPv6 accelerates the handoff procedure by using information originating from layer2. When the MN notices that it has to make a handoff,

it sends a **R**ou**t**er **Sol**icitation **Pr**oxy message (RtSolPr) to the old **A**ccess **R**outer (AR), which sends a **Pr**oxy **R**ou**t**er **Adv**ertisement message (PrRtAdv) to the MN as a response. After that, the MN sends a **F**ast **B**inding **U**pdate (F_BU) to the old AR, which builds a tunnel to the new AR to forward the MN's packets. Thus the MN will receive its packets after the handoff directly from the new AR.

An example of the fourth mobility management solutions group is **S**eamless-**M**obile **IP** (S-MIP), proposed in [16]. S-MIP reduces the required registration time by means of hierarchical network architecture and uses the layer2 information to accelerate the layer3 handoff. S-MIP introduces a new entity called **D**ecision **E**ngine (DE) to control the handoff process. When the MN reaches the boundary of the cell, it informs the current AR about the movement and about the addresses of the new discovered ARs. The current AR informs the DE and the new ARs about the movement. Following this, the movement of the MN is tracked by the DE to accurately decide to which AR the MN will move. When the DE determines the new AR it informs the old AR and the other participating ARs about the decision. Then the packets are forwarded to the old and the new AR until the DE is informed by the new AR that the MN has finished the handoff.

III- MOBILE IP FAST AUTHENTICATION PROTOCOL

MIFA [17] has been proposed in order to avoid the problems of MIP without needing to insert intermediate nodes between the FA and the HA. The basic idea of MIFA is that the HA delegates the authentication to the FA. As a result the FA authenticates the MN on behalf of the HA. Thus the MN sends **Reg**istration **R**e**q**ue**st** (Reg_Rqst) to the FA, which in turn directly replies by sending a **Reg**istration **R**e**ply** message (Reg_Rply) to the MN. After receiving the Reg_Rply, the MN can resume transmission on uplink. In downlink a tunnel is established to forward the packets, arriving at the previous FA, to the new FA until the HA is informed about the movement and a tunnel from the HA to the current FA is established to forward the packets directly to the new FA. Thus the delay experienced from the communication between the new FA and the HA is hidden from the application, similar to micro mobility protocols. Additionally the time required to build an IPSec tunnel between the HA and the FA, if needed, is avoided too.

The local authentication by FAs relies on groups of neighboring FAs. Each FA defines a set of neighboring FAs called a **L**ayer**3-F**requent **H**andoff **R**egion (L3-FHR) [18]. These

L3-FHRs can be built statically by means of standard algorithms (e.g. neighbor graph [19] or others [18]), or dynamically by the network itself, by observing the movements of the MNs. Typically, the L3-FHR of a FA consists of a small number of the FAs compared to the whole number of the FAs the MN may connect to. Every FA defines its own L3-FHR. The L3-FHR doesn't necessarily comprise all of the adjacent FAs, e.g. in the case of physical obstacles between the areas that prevent a movement between the adjacent FA areas.

There is a security association between the FAs in each L3-FHR. This security association can be established statically, e.g. by the network administrator, or dynamically, e.g. by the network itself as described in [4], [5].

Figure 1 depicts the basic operation of MIFA. While the MN communicates with the current FA, this FA sends notifications to all of the FAs in the L3-FHR the current FA belongs to. These notifications contain the necessary information required to authenticate the MN in the next registration. This information is recorded in a soft state and will be used by one of the FAs in the future and deleted from the others.

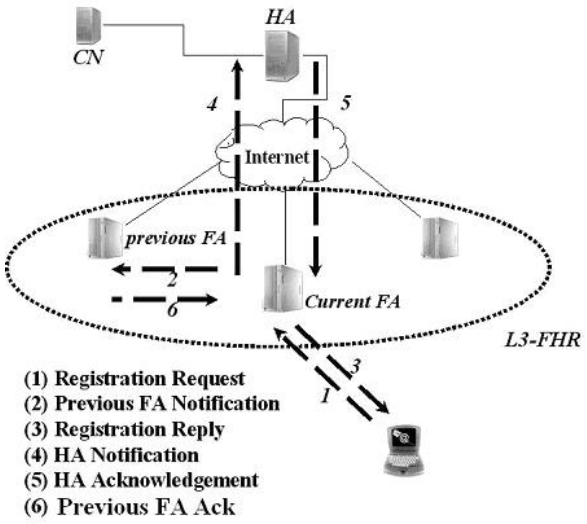

Figure 1. Basic operation of MIFA

When the MN moves to the new FA, which will be a member of the L3-FHR of the previous FA, it sends a Reg_Rqst message to this FA. The new FA authenticates the MN according to the information distributed by the notifications. If the authentication succeeds, the FA builds a **P**revious **FA Not**ification (P_FA_Not) message to inform the previous FA that it has to forward the packets, sent to the MN, to the new FA. The Previous FA acknowledges the receiving of P_FA_Not message by sending a **P**revious

FA Acknowledgement (P_FA_Ack) message and starts the forwarding to the new FA. After that the new FA sends a Reg_Reply to the MN. At this time the MN can resume transmission on uplink and downlink. Additionally the new FA sends a **HA Not**ification (HA_Not) message to inform the HA about the new binding. The HA in turn answers by sending a **HA Ack**nowledgement (HA_Ack) message to the new FA and establishes a new tunnel to the new FA.

In [20] an analytical model to evaluate the performance of MIFA compared to HMIP has been given. This analysis shows that the handoff latency of MIFA is independent of the distance between the new FA and the HA. MIFA performs similar to HMIP when the domain consists of two hierarchical levels only, i.e. a GFA at the first level and the FAs at the second level, and outperforms HMIP otherwise. The main advantage of MIFA is that it does not require hierarchical network architecture as HMIP does. Additionally, MIFA processes the handoff procedure locally without introducing any intermediate node between the FA and the HA. Thus MIFA is a protocol to manage global mobility, similar to MIP, as well as local mobility, similar to HMIP.

In [21] an analytical model to compare MIFA with HMIP with respect of location update and packet forwarding costs was introduced. This study shows that the two protocols are comparable to each other with respect to the location update cost. However, MIFA minimizes the packet delivery cost, due to avoiding the triangular routing required by HMIP (from CN to the HA, which forwards the packets to the GFA. This GFA forwards them then to the MN through the serving FA).

Micro mobility management solutions are widely deployed and well trusted. However, the movement between the different administrative domains is still processed by MIP, which causes an inadequate disruption in the communication. Thus to use the benefits of MIFA without needing to do significant changes in the domain, it is useful to integrate MIFA with the micro mobility solutions. This makes the MN able to move seamless and fast between the domains similarly as when it moves inside the same domain without restructuring and reestablishing on the domain.

VI- THE PROPOSED MOBILITY FRAMEWORK

The network architecture used in this framework is shown in figure 2. This framework uses HMIP as a micro mobility management protocol to process the handoff procedure

when the MN moves inside a certain domain. Each domain is controlled by a GFA. Each domain contains an AAA server (referred to as AAAH in the home domain and AAAF in the foreign domain). However, in order to support macro mobility between the GFAs we use MIFA instead of MIP.

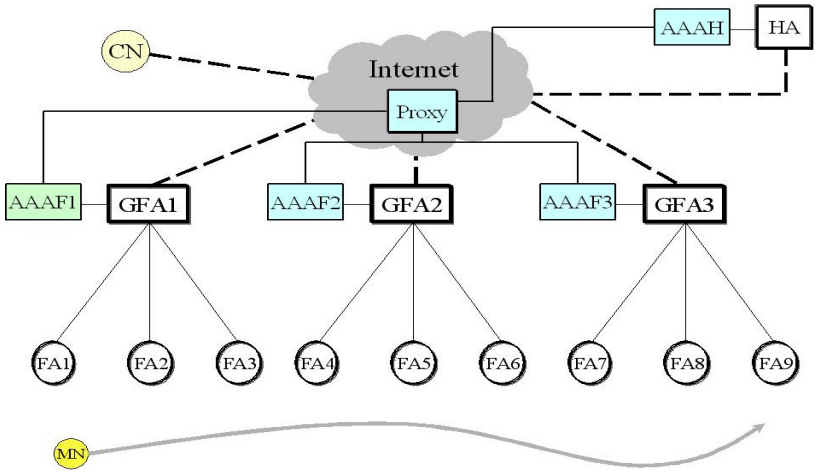

Figure 2. Network topology

a) L3-FHRs Building

L3-FHR contains the GFAs the MN may move to from a certain FA. This means, each GFA records a L3-FHR for each FA, from which the MN can move to another domain. For example, supposing that the MN can move from FA1 only to FA2 and FA3, this means that from FA1 the MN can not move outside this domain. However, from FA2 the MN can move to FA3 and FA4. FA4 belongs to another domain controlled by GFA2. Thus, the L3-FHR of FA2 will contain GFA2. A scenario for building of the L3-FHRs is depicted in table 1. The L3-FHR can be built using many methods such as neighbour graph [18] or dynamically by observing the mobility of the MNs.

Table 1. Building L3-FHRs according to movement between the FAs

Current FA	The FAs, the MN can move to	Moving outside of omain	L3-FHR
FA1	FA2, FA3	No	___
FA2	FA3, FA4	Yes	GFA2
FA3	FA2, FA4	Yes	GFA2
FA4	FA2, FA3, FA5	Yes	GFA1
FA5	FA6	No	___

FA6	FA7, FA8	Yes	GFA3
FA7	FA6, FA9	Yes	GFA2
FA8	FA6, FA9	Yes	GFA2
FA9	FA7, FA8	No	___

b) Operation of the Framework

When the MN moves into a certain domain, it registers firstly using the normal MIP procedure as depicted in figure 3. The MN sends a RegRqst message as soon as it receives an agent advertisement from this FA. Additionally, the MN informs the network infrastructure (by sending MIFA option in the RegRqst message) that it prefers to use MIFA in the next registrations. The FA then sends this message to the GFA responsible for this domain. The GFA in turn encapsulates the RegRqst in an **A**AA - **M**obile Node **R**equest message (AMR) and sends it to the AAAF server. In this AMR message the GFA has to request a FA-HA session key by including the suitable extensions defined in AAA protocols. AAAF in turn sends this message through the required proxies to the AAAH server. The AAAH server then generates a MN–FA session key ($K1_{MN\text{-}FA}$) and a MN-FA nonce. $K1_{MN\text{-}FA}$ defines the security association between the GFA and the MN. Additional to this, the AAAH generates a FA-HA session key ($K1_{FA\text{-}HA}$), which defines the security association between the GFA and the HA. A FA-HA nonce is generated too. After that it adds these new generated keys and nonces in suitable extensions to the AMR message, builds a **H**ome **A**gent MN **R**equest message (HAR) and sends it to the HA. The HA extracts the FA-HA session key and the ReqRqst message encapsulated in the HAR message and process it according to MIP procedures. After that, the HA builds a RegRply message, adds the nonces and the keys produced by the AAAH server to the message, encapsulates it in a **HA** MN **A**nswer message (HAA) and sends it to the AAAH server. The AAAH builds an **A**AA - **M**obile Node **A**nswer message (AMA) and forwards it to the AAAF server. The AAAF server in turn generates another FA-HA key ($K2_{FA\text{-}HA}$) and a MN-FA key ($K2_{MN\text{-}FA}$). $K2_{FA\text{-}HA}$ defines the security association between the HA and the new GFA the MN may move to, while $K2_{MN\text{-}FA}$ defines the security association between the MN and the new GFA, the MN may move to. Additionally, the AAAF server generates two random variables R_1, R_2 which will be used for authentication purposes in the future registration. After that it encapsulates these

new generated keys and random variables within an AMA message and forwards it to the GFA. The GFA extracts the RegRply message, $K1_{FA\text{-}HA}$, $K2_{FA\text{-}HA}$, $K1_{MN\text{-}FA}$, $K2_{MN\text{-}FA}$, R_1, R_2 and sends the RegRply message to the certain FA, which forwards it to the MN. The MN in turn extracts $K1_{MN\text{-}FA}$, $K2_{MN\text{-}FA}$, R_1 and R_2.

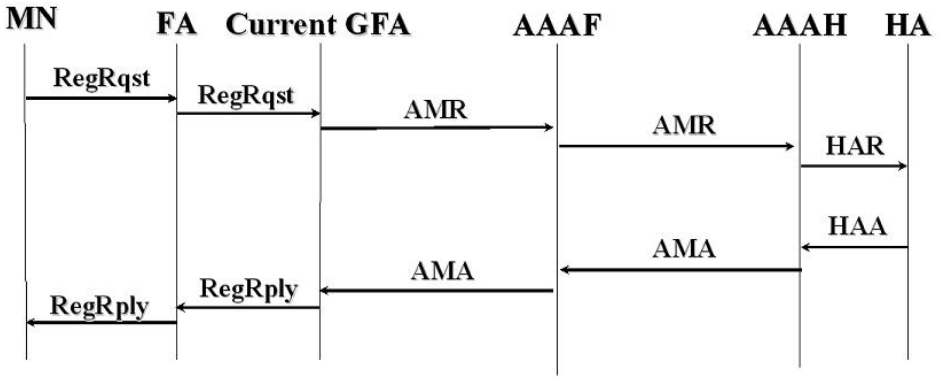

Figure 3. Initial registration

If the MN can move from this FA to other FAs belonging to other domains, the current GFA has to perform the procedures of MIFA to distribute the necessary information to the new GFAs locating in the L3-FHR of the current FA, as shown in figure 4. In order to do this, the GFA sends a **M**ove **P**robability **Not**ification message (MPNot) to the HA. This message contains the two random variables R_1, R_2 and the key $K2_{FA\text{-}HA}$ encrypted by $K1_{FA\text{-}HA}$. The HA in turn builds the authentication values $Auth_1$ and $Auth_2$, using these random variables and builds a **M**ovement **P**robability **Ack**nowledgement message (MPAck), adds $Auth_1$ and $Auth_2$ values encrypted by $K1_{FA\text{-}HA}$. Additionally, the HA adds the parameters needed by the GFA to check the replay protection and to check if the requirements asked by the MN can be satisfied. After that the MPAck message is authenticated using $K1_{FA\text{-}HA}$ and sent to the current GFA. As soon as the current GFA receives the MPAck message, it has to distribute this information to the GFAs existing in the L3-FHR of the current FA. If there are security associations between the current GFA and the GFAs in the current L3-FHR, a MPNot message containing the information received from the HA should be sent to each GFA in the L3-FHR. These messages are authenticated using the existing security associations. However, if there are no security associations between the current GFA and the neighbour GFAs, they must be built using the AAA infrastructure. In order to do this, the current GFA sends an AMR message to the AAAF controlling this domain. The current GFA asks the AAAF in this message to build security associations between this GFA and each GFA in the L3-FHR or some of them. After that the AAAF server sends an AMR message to each AAAF

server in the domains the neighboring GFAs belong to. Each AAAF server of a neighbour domain builds a security association ($K_{FA,FA}$) and answers by sending an AMA message, containing this security association between the GFA of this domain and the current GFA, to the GFA of this domain and to AAAF server of the current domain. After the security associations are built, the information needed by the neighbor GFAs to authenticate and to authorize the MN can be distributed by exchanging MPNot and MPAck messages. The security association between the GFAs in the L3-FHR must not be built for each MN, instead of this, these security associations are used to distribute the information of all of the MNs moving between these domains. Refreshing of these security associations is a task of the AAA infrastructure and transparent to MIFA.

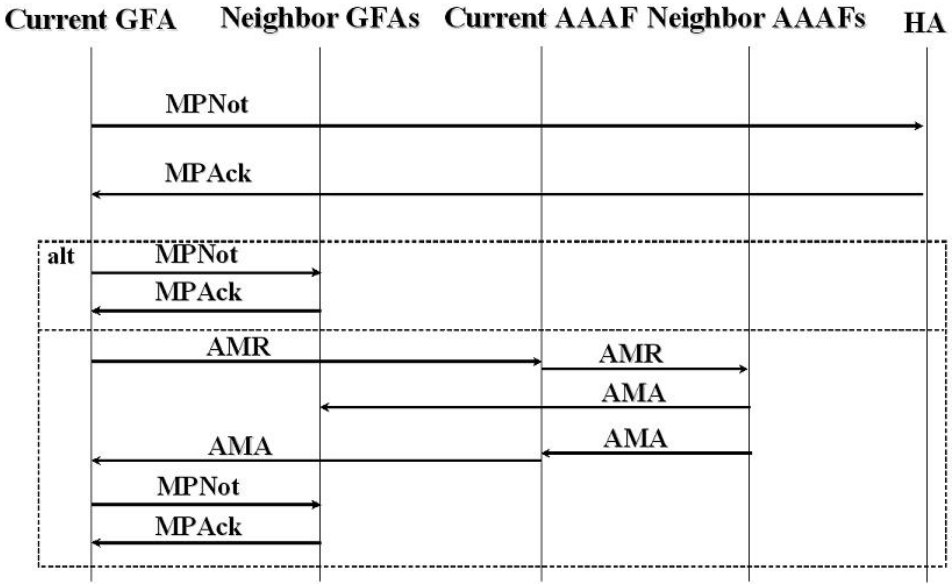

Figure 4. Exchanging and distribution of information needed for MIFA

If the MN moves to a FA locating in the same domain the previous FA belongs to, it registers itself by the GFA using the standard HMIP procedures. This means, the MN sends a **Re**g**io**nal **Reg**istration **Re**q**ue**s**t** message (RgoRegRqst) to the GFA. This message is authenticated using the security association between the GFA and the MN ($K1_{MN-FA}$) generated during the initial registration. The GFA sends a **Re**g**io**nal **Reg**istration **Re**p**ly** message (RgoRegRply) as a response. This procedure is shown in figure 5.

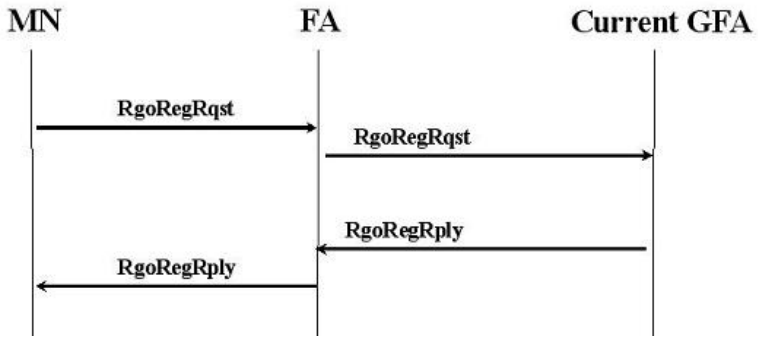

Figure 5. Regional registration

Figure 6 presents the messages exchanged when the MN changes the domain. If the MN moves outside of the domain, it has to register with the new GFA controlling this domain. This GFA has to be a member of the L3-FHR of the previous FA. Thus, the MN sends a RegRqst message to the new FA, which forwards this message to the new GFA. At first, the new GFA checks the authentication between itself and the MN. This authentication is checked employing the security association sent from the previous GFA with the notification. Subsequently, the new GFA checks MIFA information, which presents the authentication information between the MN and the HA. The new GFA then checks if the requirements requested from the HA can be satisfied. This can be done employing the attributes of the HA received with the notification, too. If all ok, the GFA builds a **P**revious **FA Not**ification message (PFANot) to inform the previous GFA that it has to forward the packets, sent to the MN, to the new GFA. After that, the new GFA generates two new random variables R_{1new} and R_{2new} for authentication purposes and another key ($K3_{MN\text{-}FA}$), which introduces the security association between the MN and the next GFA the MN may move to. A RegRply message containing this information is built and sent to the MN through the serving FA. After that, the new GFA generates another key ($K3_{FA\text{-}HA}$), which introduces the security association between the HA and the next GFA the MN may move to. After that the new GFA builds a **HA Not**ification message (HANot) containing the new generated key ($K3_{FA\text{-}HA}$) and the random variables. This message is sent to the HA to inform it about the new binding.

As soon as the previous GFA receives the PFANot message, it responds by sending a **P**revious **FA Ack**nowledgment message (PFAAck) to the new GFA. After that, all the packets the previous GFA receives with the MN as a destination are forwarded to the new GFA.

Upon receiving of HANot by the HA, it decrypts the key $K3_{FA\text{-}HA}$, extracts the random variables (R_{1new}, R_{2new}) and builds the authentication values $Auth_{1new}$ and $Auth_{2new}$ using

these random variables. After that, the HA builds a HAAck message, adds $Auth_{1new}$ and $Auth_{2new}$ values encrypted by $K2_{FA-HA}$, adds the parameters needed by the GFA to check the replay protection and to check if the MN's requirements can be satisfied by the HA, authenticates the message using $K2_{FA-HA}$ and sends it to the new GFA. After that, the HA establishes a new tunnel and tunnels the packets to the new GFA.

When the new GFA receives the HAAck message, it extracts the information existing in this message and distributes them through sending a MPNot message to each GFAs in the L3-FHR of the current FA.

Due to sending the RegRply direct from the new GFA and due to inform the previous GFA, the MN can fast resume receiving and sending of the packets. Additionally, the notification of the previous GFA enables that the time required to inform the HA about the new binding and to establish a new tunnel is hidden from the application.

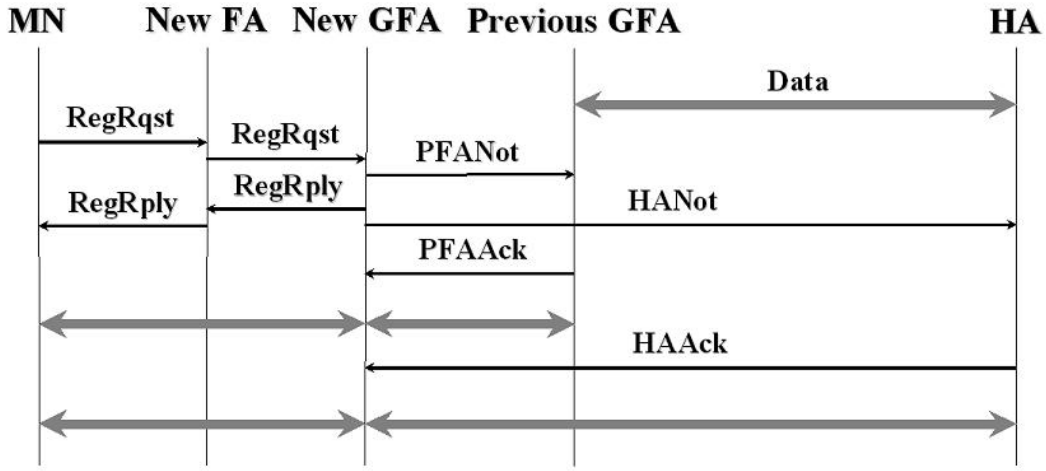

Figure 6. Inter-domain mobility

V- CONCLUSION

In the paper, we have proposed a new framework to support the mobility in All-IP networks. This framework uses HMIP to support micro mobility inside the domains and MIFA to process the movement between these domains.

Our proposed framework should outperform the standard one, which uses MIP to support mobility between the domains, with respect to the handoff latency and the expected number of dropped packets. This is because the handoff latency using the proposed framework is independent of the delay between the HA and the GFA controlling the domain. This independency achieves a fast handoff between the domains to be same as when the MN moves inside the domain.

The proposed framework introduces more security and resorts to standard one in case of failures, for example message dropping or others.

Currently, we are studying the behaviour of the proposed frame work for TCP and UDP traffic and the impact of the MN's speed on the performance.

References:

1. C.E. Perkins: MOBILE IP - Design Principles and Practices. (1998).
2. C. Perkins, Ed: IP Mobility Support for IPv4. RFC: 3344. (August 2002).
3. D. Johnson, C. Perkins, J. Arkko: Mobility Support in IPv6. RFC 3775, (2004).
4. C.E. Perkins, P.R. Calhoun: Generalized Key Distribution Extensions for Mobile IP. < draft-ietf-mobileip-gen-key-00.txt >, (2 July 2001).
5. D. B. Johnson, N. Asokan: Registration Keys for Route Optimization. < draft-ietf- mobileip-regkey-03.txt >, (14 July 2000).
6. G. Dommety, Tao Ye: Local and Indirect Registration for Anchoring Handoffs. < draft-dommety-mobileip-anchor-handoff-01.txt >, (July 2000).
7. C. E. Perkins, K. Y. Wang: Optimized Smooth Handoffs in Mobile IP. Proceedings of the Fourth IEEE Symposium on Computers and Communications, (July 1999).
8. E. Gustafsson, A. Jonsson, Charles E. Perkins: Mobile IPv4 Regional Registration. < draft-ietf-mobileip-reg-tunnel-08.txt >, (November 2003).
9. H. Soliman, C. Castelluccia, K. El-Malki, L. Bellier: Hierarchical Mobile IPv6 mobility management (HMIPv6). < draft-ietf-mobileip-hmipv6-08.txt >, (June 2003).
10. K. El Malki et al.: Low Latency Handoffs in Mobile IPv4. <draft-ietf-mobileip-lowlatency-handoffs-v4-04.txt>, (June 2002).
11. C. Blondia, O. Casals, Ll. Cerdà, N. Van den Wijngaert, G. Willems, P. De Cleyn: Low Latency Handoff Mechanisms and Their Implementation in an IEEE 802.11 Network. Proceedings of ITC18, Berlin, Germany, (2003).
12. O. Casals, et al: Performance Evaluation of the Post-Registration Method, a Low Latency Handoff in MIPv4. Proceedings of IEEE 2003 International Confernence on Communications, ICC 2003, Anchorage, (May 2003).
13. C. Blondia, O. Casals, Ll. Cerdà, N. Van den Wijngaert, G. Willems, P. De Cleyn: Performance Comparison of Low Latency Mobile IP Schemes. Proceedings at WiOpt'03 Modeling and Optimization in Mobile Ad Hoc and Wireless Networks, INRIA, Sophia Antipolis, pp. 115-124, (March 2003).
14. Shiva Raman Pandey, Satish Jamadagni: Improved Low Latency Handoff in Mobile IPv4. <draft-shiva-improved-lowlatency-handoff-v4-01.txt>, (February 2002).
15. R. Koodli, Fast Handovers for Mobile IPv6, Internet draft, July 2004.
16. R. Hsieh, Z. G. Zhou, A. Seneviratne: S-MIP: A Seamless Handoff Architecture for Mobile IP. In Proceedings of INFOCOM, San Francisco, USA (2003).
17. A. Diab, A. Mitschele-Thiel: Minimizing Mobile IP Handoff Latency. 2nd International Working Conference on Performance modelling and Evaluation of Heterogeneous Networks , HET-NETs'04, Ilkley, West Yorkshire, U.K., (July 2004).
18. S. Pack, Y. Choi: Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN. Networks 2002, (August 2002).
19. S.K. Sen, et al.: A Selective Location Update Strategy for PCS Users. ACM/Baltzer J. Wireless Networks, (September 1999).
20. A. Diab, A. Mitschele-Thiel, J. Xu: Perfomance Analysis of the Mobile IP Fast Authentication Protocol. Seventh ACM Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2004), Venice, Italy, (October 2004).
21. A. Diab, A. Mitschele-Thiel, R. Böringer: Evaluation of Mobile IP Fast Authentication Protocol compared to Hierarchical Mobile IP. IEEE Conference on Wireless and Mobile Computing, Networking and Communications WiMob'2005, Montreal, (August 2005).

Authors:

Dipl.-Ing Ali Diab
Prof. Dr.-Ing. habil. Andreas Mitschele-Thiel
Dipl.-Ing René Böringer
TU - Ilmenau, Faculty for Informatics und Automation, Gustav-Kirchhoff-Str. 1, P.O.B. 10 0565
98693, Ilmenau
Phone: +49 3677 69 2819
Fax: +49 3677 69 1220
E-mail: {ali.diab|mitsch|rene.boeringer}@tu-ilmenau.de